PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-083138
(43)Date of publication of application : 31.03.1998

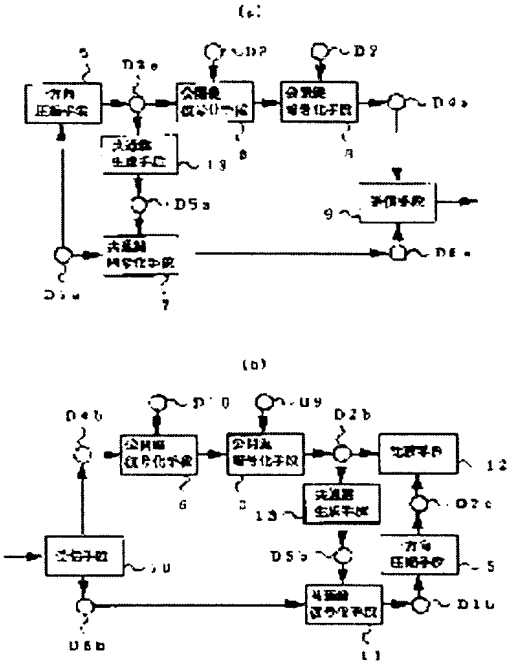
(51)Int.Cl. G09C 1/00
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 08-236528
(22)Date of filing : 06.09.1996

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : HARA YOSHIAKI

(54) DATA TRANSMISSION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate a common key controlling work when a transmitter transmits data to a receiver excepting a transmitter oneself by a common key ciphering transmission data and to automatically generating a common key required for a concealing for a third person from data.
SOLUTION: When the transmitter transmits the data to the receiver excepting the transmitter oneself, that is, when the open key of the receiver is different from the open key of the transmitter, transmitted signature D4a becomes the contents different from a summary D2a becoming the origin generating the open key D5a. Then, even when the third person having no secret key D10 of the receiver intercepts the signature and the ciphered data while transmitting, the third person can't open key decipher the signature by the secret key D10 of the receiver to can't generate the summary. Thus, since the common key isn't generated from the summary, and the ciphered data aren't common key deciphered, and the data aren't obtained, the contents of the data D1a are concealed for the third person. That is, the attestation of the receiver intended by the transmitter is performed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－83138

(43)公開日　平成10年(1998)３月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｃ
		7259－5Ｊ		６３０Ｅ
	６４０	7259－5Ｊ		６４０Ｂ
		7259－5Ｊ		６４０Ｄ
		7259－5Ｊ		６４０Ｅ

審査請求　未請求　請求項の数８　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願平8－236528

(22)出願日　平成８年(1996)９月６日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　原　嘉明
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

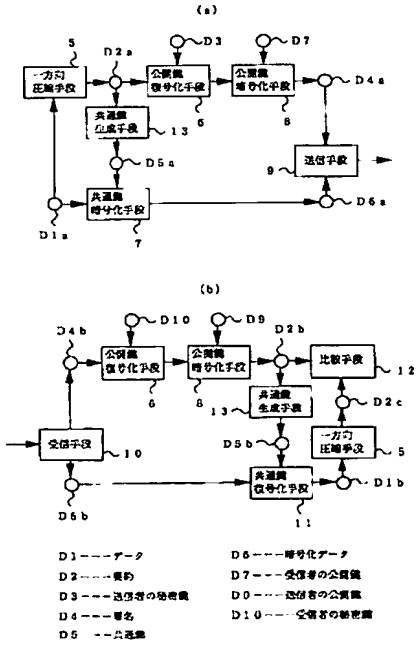
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】　データ伝送方法

(57)【要約】

【課題】　データの秘匿、送受信者の相互認証、データの一貫性の保証が可能なデータ伝送方法において、共通鍵の管理を不要とする。

【解決手段】　データを一方向圧縮した要約から共通鍵を自動的に生成してデータを共通鍵暗号化し、要約を送信者のみか組み立てられ、かつ受信者のみか翻訳できる署名として送信し、受信した署名から共通鍵を生成してデータを共通鍵復号化し、また署名から生成した要約とデータから生成した要約を比較し、送受信者の相互認証およびデータの一貫性を判定する。



1

【特許請求の範囲】

【請求項１】　複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を送信者の第１の秘密鍵で公開鍵復号化したのち受信者の第１の公開鍵で署名に公開鍵暗号化し、かつ前記要約に基つき第１の共通鍵を生成し、前記所定のデータを前記第１の共通鍵で暗号化データに共通鍵暗号として、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、前記署名を受信者の第２の秘密鍵で公開鍵復号化したのち送信者の第２の公開鍵で要約に公開鍵暗号化し、この要約に基づいて第２の共通鍵を生成し、前記受信された暗号化データを前記第２の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項２】　複数のデータ伝送装置か伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を受信者の第１の公開鍵で公開鍵暗号化したのち送信者の第１の秘密鍵で署名に公開鍵復号化し、かつ前記要約に基つき第１の共通鍵を生成し、前記所定のデータを前記第１の共通鍵で暗号化データに共通鍵暗号化して、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を送信者の第２の公開鍵で公開鍵暗号化したのち受信者の第２の秘密鍵て要約に公開鍵復号化し、この要約に基づいて第２の共通鍵を生成し、前記受信された暗号化データを前記第２の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項３】　複数のデータ伝送装置か伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を送信者の第１の秘密鍵で公開鍵復号化したのち受信者の第１の公開鍵で二重に公開鍵暗号化して署名を生成し、前記要約に基つき第１の共通鍵を生成し、前記所定のデータを前記第１の共通鍵て暗号化データに共通鍵暗号化して、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第２の秘密鍵て二重に公開鍵復号化したのち送信者の第２の公開鍵で要約に公開鍵暗号化し、この要約に基ついて第２の共通鍵を生成し、前記受

2

信された暗号化データを前記第２の共通鍵てデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定手順とを有することを特徴とするデータ伝送方法。

【請求項４】　複数のデータ伝送装置か伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を受信者の第１の公開鍵て公開鍵暗号化したのち送信者の第１の秘密鍵て公開鍵復号化し、さらに受信者の第１の公開鍵て署名に公開鍵暗号化し、前記要約に基ついて第１の共通鍵に生成し、前記所定のデータを前記第１の共通鍵て暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第２の秘密鍵て公開鍵復号化したのち送信者の第２の公開鍵て公開鍵暗号化し、さらに受信者の第２の秘密鍵て要約に公開鍵復号化し、この要約に基ついて第２の共通鍵を生成し、前記受信された暗号化データを前記第２の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成された要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項５】　複数のデータ伝送装置が伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を受信者の第１の公開鍵て二重に公開鍵暗号化したのち送信者の第１の秘密鍵で署名に公開鍵復号化し、前記要約に基ついて第１の共通鍵を生成し、前記テータを前記第１の共通鍵で暗号化データに共通鍵暗号化して前記暗号化テータと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を送信者の第２の公開鍵て公開鍵暗号化したのち受信者の第２の秘密鍵て二重に公開鍵復号化して要約を生成し、この要約により共通鍵を生成し、前記受信された暗号化テータを第２の共通鍵てテータに共通鍵復号化し、このテータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項６】　複数のデータ伝送装置か伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を送信者の第１の秘密鍵て中間署名に公開鍵復号化し、この中間署名を受信者の第１の公開鍵て署名に公開

鍵暗号化し、前記中間署名により第１の共通鍵を生成し、前記データを前記第１の共通鍵で暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第２の秘密鍵で中間署名に公開鍵復号化し、この中間署名を送信者の第２の公開鍵で要約に公開鍵暗号化し、前記中間署名により第２の共通鍵に生成し、前記受信された暗号化データを第２の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項７】　複数のデータ伝送装置か伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を送信者の第１の秘密鍵で公開鍵復号化したのち受信者の第１の公開鍵で中間署名に公開鍵暗号化し、この中間署名を受信者の第１の公開鍵て署名に公開鍵暗号化し、前記中間署名により第１の共通鍵を生成し、前記データを第１の共通鍵で暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第２の秘密鍵で中間署名に公開鍵復号化し、この中間署名を受信者の第２の秘密鍵で公開鍵復号化したのち送信者の第２の公開鍵て要約に公開鍵暗号化し、前記中間署名により第２の共通鍵を生成し、前記受信された暗号化データを第２の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項８】　複数のデータ伝送装置か伝送路により接続されて成るネットワーク上て、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を受信者の第１の公開鍵で公開鍵暗号化したのち送信者の第１の秘密鍵で中間署名に公開鍵復号化し、この中間署名を受信者の第１の公開鍵て署名に公開鍵暗号化し、前記中間署名により第１の共通鍵を生成し、前記データを第１の共通鍵で暗号化データに共通鍵暗号化して、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第２の秘密鍵で中間署名に公開鍵復号化し、この中間署名を送信者の第２の公開鍵て公開鍵暗号化したのち受信者の第２の秘密鍵て要約に公開鍵復号化し、前記中間署名により第２の共通鍵を生成し、前記受信された暗号化データを第２の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定する手順とを有することを特徴とするデータ伝送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、伝送データの第三者に対する秘匿、送受信者の相互認証、およびデータの一貫性の保証すなわちデータか改さんされていないことの保証を可能とするデータ伝送方法に関する。

【０００２】

【従来の技術】例えば電子メールのようなデータ伝送によって、商取引のデータなどを安全に伝送するためには、伝送データの第三者に対する秘匿、送受信者の相互認証およびデータの一貫性の保証をする必要がある。このため、伝送データの秘匿のために、公開鍵暗号より高速な処理ができる共通鍵暗号を利用し、該共通鍵暗号の共通鍵の秘匿及び送受信者の相互認証のために公開鍵暗号を利用したデータ伝送方法か従来から用いられている。

【０００３】図１１はこのようなデータ伝送方法が適用されるデータ伝送の説明図であり、１はデータの送信者、２は送信者１の意図するデータの受信者、３は送信者１および受信者２以外の第三者、４はデータの伝送路てある。送信者１か受信者２に伝えようとするデータは、送信者１のみか組み立てられ、かつ受信者２のみか翻訳できる形式に変換されて伝送路４を介して伝送される。

【０００４】図１２は前記従来のデータ伝送方法の説明図、図１３は前記従来のデータ伝送方法のフローチャートである。図１２および図１３において（ａ）は送信者側、（ｂ）が受信者側の説明図およびフローチャートてある。図１２（ａ）において、送信者１が受信者２に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは送信者の秘密鍵Ｄ３て公開鍵復号化手段６により署名Ｄ４ａに公開鍵復号化される（処理Ｓ２）。前記データＤ１ａは、送信者により送信のたひに「ＡｂｃＤ」や「ｗＸｙＺ」なとのように人力された共通鍵Ｄ５ａて共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記共通鍵Ｄ５ａは受信者の公開鍵Ｄ７て公開鍵暗号化手段８により暗号化共通鍵Ｄ８ａに公開鍵暗号化される（処理Ｓ４）。前記署名Ｄ４ａ、前記暗号化データＤ６ａおよび該暗号化共通鍵Ｄ８ａは送信手段９により送信され（処理Ｓ５）、図１２（ｂ）において、受信手段１０により署名Ｄ４ｂ、暗号化データＤ６ｂおよび暗号化共通鍵Ｄ８ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは送信者の公開鍵Ｄ９て公開鍵暗号化手段８により要約

Ｄ２ｂに公開鍵暗号化される（処理Ｓ７）。前記暗号化共通鍵Ｄ８ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により共通鍵Ｄ５ｂに公開鍵復号化される（処理Ｓ８）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂで共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証かされたと判定される。

【０００５】以上のような従来のデータ伝送方法において、受信者の秘密鍵Ｄ１０を持たない第三者３か伝送中の署名、暗号化データおよび暗号化共通鍵を傍受しても、暗号化共通鍵を受信者の秘密鍵Ｄ１０で公開鍵復号化して共通鍵を得ることかできず、暗号化データを共通鍵で共通鍵復号化してデータを得ることかてきないため、データＤ１ａの内容は第三者３に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者１か意図する受信者２のみてあり、受信者の認証がなされる。

【０００６】また、送信者の秘密鍵Ｄ３を持たない第三者３かデータを改さんしても、改さんしたテータを一方向圧縮した要約を送信者の秘密鍵Ｄ３で署名に公開鍵復号化することかできない。このため、第三者３か改さんした署名、暗号化データおよび暗号化共通鍵を受信者２が受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれは、送信者の認証およびデータの一貫性の保証かされたと判定できる。このようにして、伝送テータの第三者に対する秘匿、送受信者の相互認証およびテータの一貫性の保証かなされる。

【０００７】

【発明か解決しようとする課題】前記従来のデータ伝送方法ては、伝送テータを第三者に対して秘匿するためには、送信者は少なくとも受信者ごとに異なりかつ第三者には推定しにくい共通鍵を準備し、共通鍵を第三者に対して秘匿し、また第三者による共通鍵推定の試みか成功する危険に備えて、頻繁に共通鍵を変更するなどの管理か必要て、そのため共通鍵の管理のための作業負担か大きいなどの問題点かあった。

【０００８】この発明の目的は、このような課題を解決するためになされたものであって、共通鍵の管理を不要とすることによって、共通鍵の管理作業の必要をなくしたデータ伝送方法を提供することにある。

【０００９】

【課題を解決するための手段】第１の発明に係るテータ伝送方法は、送信者のデータ伝送装置により、テータを要約に一方向圧縮し、該要約を送信者の秘密鍵て公開鍵

復号化したのち受信者の公開鍵て署名に公開鍵暗号化し、前記要約を共通鍵に変換し、前記データを該共通鍵て暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のテータ伝送装置により、送信者のテータ伝送装置から送信された暗号化テータと署名とを受信し、該署名を受信者の秘密鍵て公開鍵復号化したのち送信者の公開鍵て要約に公開鍵暗号化し、該要約を共通鍵に変換し、前記受信された暗号化テータを該共通鍵てデータに共通鍵復号化し、該データを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびテータの一貫性の保証かされたと判定する。

【００１０】第２の発明に係るデータ伝送方法は、送信者のテータ伝送装置により、テータを要約に一方向圧縮し、該要約を受信者の公開鍵て公開鍵暗号化したのち送信者の秘密鍵て署名に公開鍵復号化し、前記要約を共通鍵に変換し、前記データを該共通鍵て暗号化テータに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を送信者の公開鍵て公開鍵暗号化したのち受信者の秘密鍵で要約に公開鍵復号化し、該要約を共通鍵に変換し、前記受信された暗号化テータを該共通鍵でデータに共通鍵復号化し、該テータを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびテータの一貫性の保証かされたと判定する。

【００１１】第３の発明に係るテータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方向圧縮し、該要約を送信者の秘密鍵て公開鍵復号化したのち受信者の公開鍵て二重に公開鍵暗号化して署名を生成し、前記要約を共通鍵に変換し、前記データを該共通鍵て暗号化データに共通鍵暗号化し、該暗号化テータと前記署名とを送信し、受信者のデータ伝送装置により、送信者のテータ伝送装置から送信された暗号化テータと署名とを受信し、該署名を受信者の秘密鍵で二重に公開鍵復号化したのち送信者の公開鍵て要約に公開鍵暗号化し、該要約を共通鍵に変換し、前記受信された暗号化テータを該共通鍵てデータに共通鍵復号化し、該テータを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびテータの一貫性の保証かされたと判定する。

【００１２】第４の発明に係るテータ伝送方法は、送信者のデータ伝送装置により、テータを要約に一方向圧縮し、該要約を受信者の公開鍵て公開鍵暗号化したのち送信者の秘密鍵て公開鍵復号化し、さらに受信者の公開鍵て署名に公開鍵暗号化し、前記要約を共通鍵に変換し、前記データを該共通鍵て暗号化テータに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のテータ伝送装置により、送信者のテータ伝送装置から送信

された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で公開鍵復号化したのち送信者の公開鍵で公開鍵暗号化し、さらに受信者の秘密鍵で要約に公開鍵復号化し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定する。

【００１３】第５の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方向圧縮し、該要約を受信者の公開鍵で二重に公開鍵暗号化したのち送信者の秘密鍵で署名に公開鍵復号化し、前記要約を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を送信者の公開鍵で公開鍵暗号化したのち受信者の秘密鍵で二重に公開鍵暗号化して要約を生成し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定することを特徴とするデータ伝送方法。

【００１４】第６の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方向圧縮し、該要約を送信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を受信者の公開鍵で署名に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を送信者の公開鍵で要約に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定することを特徴とするデータ伝送方法。

【００１５】第７の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方向圧縮し、該要約を送信者の秘密鍵で公開鍵復号化したのち受信者の公開鍵で中間署名に公開鍵暗号化し、該中間署名を受信者の公開鍵で署名に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を受信者の秘密鍵で公開鍵復号化したのち送信者の公開鍵で要約に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証かされたと判定することを特徴とするデータ伝送方法。

【００１６】第８の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方向圧縮し、該要約を受信者の公開鍵で公開鍵暗号化したのち送信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を受信者の公開鍵で署名に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を送信者の公開鍵で公開鍵暗号化したのち受信者の秘密鍵で要約に公開鍵復号化し、前記中間署名を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定することを特徴とするデータ伝送方法。

【００１７】

【発明の実施の形態】

実施の形態１．図１はこの発明によるデータ伝送方法の実施の形態１の説明図、図２はこの発明によるデータ伝送方法の実施の形態１のフローチャートである。図１および図２において（ａ）は送信者側、（ｂ）か受信者側の説明図およびフローチャートてある。図１（ａ）において、送信者か受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは送信者の秘密鍵Ｄ３て公開鍵復号化手段６により公開鍵復号化されたのち受信者の公開鍵Ｄ７で公開鍵暗号化手段８により署名Ｄ４ａに公開鍵暗号化される（処理Ｓ２）。前記要約Ｄ２ａは、例えば先頭の２ハイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１１）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図１（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは受信者の秘密鍵Ｄ１０て公開鍵復号化手段６により公開鍵復号化されたのち送信者の公開鍵Ｄ９て公開鍵

暗号化手段８により要約Ｄ２ｂに公開鍵暗号化される（処理Ｓ７）。該要約Ｄ２ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１１）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂて共通鍵復号化手段１１によりテータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該テータＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者か一致すれば送受信者の相互認証およびデータの一貫性の保証かされたと判定される。

【００１８】以上のような実施の形態１のデータ伝送方法において、送信者か送信者自身以外の受信者に対してデータ伝送を行った場合、すなわち受信者の公開鍵が送信者の公開鍵と異なる場合、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる要約Ｄ２ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者が伝送中の署名および暗号化テータを傍受しても、署名を受信者の秘密鍵Ｄ１０て公開鍵復号化することができず、要約を生成できない。したかって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してテータを得ることかてきないため、テータＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したテータＤ１ｂを翻訳できるのは、送信者か意図する受信者のみであり、受信者の認証かなされる。

【００１９】また、送信者の秘密鍵Ｄ３を持たない第三者かテータを改さんしても、改さんしたテータを一方向圧縮した要約を送信者の秘密鍵Ｄ３て公開鍵復号化することかてきず、署名を生成できない。このため、第三者が改さんした署名および暗号化データを受信者が受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータ Ｄ１ｂから生成した要約Ｄ２ｃか一致すれば、送信者の認証およびテータの一貫性の保証かされたと判定てきる。

【００２０】実施の形態２．図３はこの発明によるデータ伝送方法の実施の形態２の説明図、図２はこの発明によるテータ伝送方法の実施の形態２のフローチャートである。図３および図２において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートである。図３（ａ）において、送信者か受信者に伝えようとするテータＤ１ａは例えはハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは受信者の公開鍵Ｄ７て公開鍵暗号化手段８により公開鍵暗号化されたのち送信者の秘密鍵Ｄ３て公開鍵復号化手段６により署名Ｄ４ａに公開鍵復号化される（処理Ｓ２）。前記要約Ｄ２ａは、例えは先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１１）。前記テータＤ１ａは該共通鍵Ｄ５ａて共通鍵暗号化手段７により暗号化テータＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化テータＤ６ａは送信手段９により送信され（処理Ｓ５）、図３（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化テータＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは送信者の公開鍵Ｄ９て公開鍵暗号化手段８により公開鍵暗号化されたのち受信者の秘密鍵Ｄ１０て公開鍵復号化手段６により要約Ｄ２ｂに公開鍵復号化される（処理Ｓ７）。該要約Ｄ２ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１１）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂて共通鍵復号化手段１１によりテータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該テータＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｓ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者か一致すれば送受信者の相互認証およびデータの一貫性の保証かされたと判定される。

【００２１】以上のような実施の形態２のデータ伝送方法において、送信者が送信者自身以外の受信者に対してデータ伝送を行った場合、すなわち受信者の公開鍵が送信者の公開鍵と異なる場合、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる要約Ｄ２ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者か伝送中の署名および暗号化データを傍受し、署名を送信者の公開鍵Ｄ９で公開鍵暗号化しても、受信者の秘密鍵Ｄ１０で公開鍵復号化することかてきず、要約を生成てきない。したかって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることができないため、テータＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証がなされる。

【００２２】また、送信者の秘密鍵Ｄ３を持たない第三者かデータを改さんし、改さんしたテータを一方向圧縮した要約を受信者の公開鍵Ｄ７て公開鍵暗号化しても、送信者の秘密鍵Ｄ３て公開鍵復号化することかてきず、署名を生成できない。このため、第三者が改さんした署名および暗号化テータを受信者か受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したテータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれば、送信者の認証およびデータの一貫性の保証かされたと判定てきる。

【００２３】実施の形態３．図４はこの発明によるテータ伝送方法の実施の形態３の説明図、図２はこの発明によるデータ伝送方法の実施の形態３のフローチャートである。図４および図２において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートてあ

る。図４（ａ）において、送信者が受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは送信者の秘密鍵Ｄ３で公開鍵復号化手段６により公開鍵復号化されたのち受信者の公開鍵Ｄ７で公開鍵暗号化手段８により二重に公開鍵暗号化され、署名Ｄ４ａが生成される（処理Ｓ２）。前記要約Ｄ２ａは、例えば先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１１）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図４（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により二重に公開鍵復号化されたのち送信者の公開鍵Ｄ９で公開鍵暗号化手段８により要約Ｄ２ｂに公開鍵暗号化される（処理Ｓ７）。該要約Ｄ２ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１１）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂで共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｓ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【００２４】以上のような実施の形態３のデータ伝送方法において、送信者が送信者自身に対してデータ伝送を行った場合でも、すなわち受信者の公開鍵が送信者の公開鍵とおなじ場合でも、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる要約Ｄ２ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵Ｄ１０で公開鍵復号化することができず、要約を生成できない。したかって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかできないため、データＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者が意図する受信者のみてあり、受信者の認証かなされる。

【００２５】また、送信者の秘密鍵Ｄ３を持たない第三者かデータを改さんしても、改さんしたデータを一方向圧縮した要約を送信者の秘密鍵Ｄ３て公開鍵復号化することかてきず、署名を生成できない。このため、第三者か改さんした署名および暗号化データを受信者か受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれは、送信者の認証およびデータの一貫性の保証かされたと判定できる。

【００２６】実施の形態４．図５はこの発明によるデータ伝送方法の実施の形態４の説明図、図２はこの発明によるデータ伝送方法の実施の形態４のフローチャートてある。図５および図２において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートである。図５（ａ）において、送信者か受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは受信者の公開鍵Ｄ７で公開鍵暗号化手段８により公開鍵暗号化されたのち送信者の秘密鍵Ｄ３で公開鍵復号化手段６により公開鍵復号化され、さらに受信者の公開鍵Ｄ７で公開鍵暗号化手段８により署名Ｄ４ａに公開鍵暗号化される（処理Ｓ２）。前記要約Ｄ２ａは、例えば先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１１）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図５（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により公開鍵復号化されたのち送信者の公開鍵Ｄ９で公開鍵暗号化手段８により公開鍵暗号化され、さらに受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により要約Ｄ２ｂに公開鍵復号化される（処理Ｓ７）。該要約Ｄ２ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１１）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂで共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【００２７】以上のような実施の形態４のデータ伝送方法において、送信者か送信者自身に対してデータ伝送を行った場合でも、すなわち受信者の公開鍵か送信者の公開鍵とおなじ場合でも、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる要約Ｄ２ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵Ｄ１０で公開鍵復号化することかできず、要約を生成できない。したかって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかてきないため、データＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳

できるのは、送信者か意図する受信者のみてあり、受信者の認証かなされる。

【００２８】また、送信者の秘密鍵Ｄ３を持たない第三者かテータを改さんし、改さんしたテータを一方向圧縮した要約を受信者の公開鍵Ｄ７て公開鍵暗号化しても、送信者の秘密鍵Ｄ３て公開鍵復号化することかできす、署名を生成てきない。このため、第三者か改さんした署名および暗号化テータを受信者か受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【００２９】実施の形態５．図６はこの発明によるデータ伝送方法の実施の形態５の説明図、図２はこの発明によるデータ伝送方法の実施の形態５のフローチャートである。図６および図２において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートである。図６（ａ）において、送信者が受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは受信者の公開鍵Ｄ７で公開鍵暗号化手段８により二重に公開鍵暗号化されたのち送信者の秘密鍵Ｄ３で公開鍵復号化手段６により署名Ｄ４ａに公開鍵復号化される（処理Ｓ２）。前記要約Ｄ２ａは、例えば先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１１）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図６（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは送信者の公開鍵Ｄ９で公開鍵暗号化手段８により公開鍵暗号化されたのち受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により二重に公開鍵復号化され、要約Ｄ２ｂが生成される（処理Ｓ７）。該要約Ｄ２ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１１）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂて共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者か一致すれば送受信者の相互認証およびデータの一貫性の保証かされたと判定される。

【００３０】以上のような実施の形態５のテータ伝送方法において、送信者が送信者自身に対してデータ伝送を行った場合でも、すなわち受信者の公開鍵か送信者の公開鍵とおなじ場合でも、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる要約Ｄ２ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者か伝送中の署名および暗号化テータを傍受し、署名を送信者の公開鍵Ｄ９て公開鍵暗号化しても、受信者の秘密鍵Ｄ１０て公開鍵復号化することかてきす、要約を生成できない。したかって、要約から共通鍵を生成し、暗号化テータを共通鍵復号化してデータを得ることかできないため、データＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者か意図する受信者のみであり、受信者の認証かなされる。また、送信者の秘密鍵Ｄ３を持たない第三者かテータを改ざんし、改ざんしたデータを一方向圧縮した要約を受信者の公開鍵Ｄ７で公開鍵暗号化しても、送信者の秘密鍵Ｄ３で公開鍵復号化することかできす、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【００３１】実施の形態６．図７はこの発明によるデータ伝送方法の実施の形態６の説明図、図８はこの発明によるデータ伝送方法の実施の形態６のフローチャートである。図７および図８において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートである。図７（ａ）において、送信者が受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは送信者の秘密鍵Ｄ３で公開鍵復号化手段６により中間署名Ｄ１１ａに公開鍵復号化され（処理Ｓ１２）、該中間署名Ｄ１１ａは受信者の公開鍵Ｄ７で公開鍵暗号化手段８により署名Ｄ４ａに公開鍵暗号化される（処理Ｓ１３）。前記中間署名Ｄ１１ａは、例えば先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１４）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図７（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により中間署名Ｄ１１ｂに公開鍵復号化され（処理Ｓ１５）、該中間署名Ｄ１１ｂは送信者の公開鍵Ｄ９て公開鍵暗号化手段８により要約Ｄ２ｂに公開鍵暗号化される（処理Ｓ１６）。前記中間署名Ｄ１１ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変

換される（処理Ｓ１４）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂで共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証かされたと判定される。

【００３２】以上のような実施の形態６のデータ伝送方法において、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる中間署名Ｄ１１ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者か伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵Ｄ１０で中間署名に公開鍵復号化することができず、要約を生成できない。したかって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることができないため、データＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者か意図する受信者のみであり、受信者の認証がなされる。

【００３３】また、送信者の秘密鍵Ｄ３を持たない第三者がデータを改ざんし、改ざんしたデータを一方向圧縮した要約を送信者の秘密鍵Ｄ３で中間署名に公開鍵復号化することができず、署名を生成できない。このため第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれば、送信者の認証およびデータの一貫性の保証かされたと判定できる。

【００３４】実施の形態７．図９はこの発明によるデータ伝送方法の実施の形態７の説明図、図８はこの発明によるデータ伝送方法の実施の形態７のフローチャートである。図９および図８において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートである。図９（ａ）において、送信者か受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは送信者の秘密鍵Ｄ３で公開鍵復号化手段６により公開鍵復号化されたのち受信者の公開鍵Ｄ７で公開鍵暗号化手段８により中間署名Ｄ１１ａに公開鍵暗号化され（処理Ｓ１２）、該中間署名Ｄ１１ａは受信者の公開鍵Ｄ７で公開鍵暗号化手段８により署名Ｄ４ａに公開鍵暗号化される（処理Ｓ１３）。前記中間署名Ｄ１１ａは、例えば先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１４）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図９（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）、該署名Ｄ４ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により中間署名Ｄ１１ｂに公開鍵復号化され（処理Ｓ１５）、該中間署名Ｄ１１ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により公開鍵復号化されたのち送信者の公開鍵Ｄ９で公開鍵暗号化手段８により要約Ｄ２ｂに公開鍵暗号化される（処理Ｓ１６）。前記中間署名Ｄ１１ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１４）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂで共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証かされたと判定される。

【００３５】以上のような実施の形態７のデータ伝送方法において、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる中間署名Ｄ１１ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵Ｄ１０で中間署名に公開鍵復号化することができず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかできないため、データＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証がなされる。さらに、同一内容のデータを複数の受信者に対して伝送する場合、すなわち複数の受信者の公開鍵が互いに異なる場合は、中間署名Ｄ１１ａは受信者ごとに異なる内容で生成されるため、中間署名Ｄ１１ａから生成される共通鍵Ｄ５ａも受信者ごとに異なり、したかって、共通鍵Ｄ５ａで共通鍵暗号化手段７により生成される暗号化データＤ６ａも受信者ごとに異なる。

【００３６】また、送信者の秘密鍵Ｄ３を持たない第三者かデータを改ざんしても、改ざんしたデータを一方向圧縮した要約を送信者の秘密鍵Ｄ３で公開鍵復号化することができず、中間署名を生成できないため、署名を生成できない。このため、第三者が改さんした署名および暗号化データを受信者か受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれば、送信者の認証およびデータの一貫性の保証かされたと判定できる。

【００３７】実施の形態８．図１０はこの発明によるテ

ータ伝送方法の実施の形態８の説明図、図８はこの発明によるデータ伝送方法の実施の形態８のフローチャートである。図１０および図８において（ａ）は送信者側、（ｂ）は受信者側の説明図およびフローチャートである。図１０（ａ）において、送信者か受信者に伝えようとするデータＤ１ａは例えばハッシュ法による一方向圧縮手段５により要約Ｄ２ａに一方向圧縮され（処理Ｓ１）、該要約Ｄ２ａは受信者の公開鍵Ｄ７で公開鍵暗号化手段８により公開鍵暗号化されたのち送信者の秘密鍵Ｄ３で公開鍵復号化手段６により中間署名Ｄ１１ａに公開鍵復号化され（処理Ｓ１２）、該中間署名Ｄ１１ａは受信者の公開鍵Ｄ７で公開鍵暗号化手段８により署名Ｄ４ａに公開鍵暗号化される（処理Ｓ１３）。前記中間署名Ｄ１１ａは、例えば先頭の２バイト分を１６進数表記の４文字に変換するといった共通鍵生成手段１３により共通鍵Ｄ５ａに変換される（処理Ｓ１４）。前記データＤ１ａは該共通鍵Ｄ５ａで共通鍵暗号化手段７により暗号化データＤ６ａに共通鍵暗号化される（処理Ｓ３）。前記署名Ｄ４ａおよび該暗号化データＤ６ａは送信手段９により送信され（処理Ｓ５）、図１０（ｂ）において、受信手段１０により署名Ｄ４ｂおよび暗号化データＤ６ｂとして受信される（処理Ｓ６）。該署名Ｄ４ｂは受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により中間署名Ｄ１１ｂに公開鍵復号化され（処理Ｓ１５）、該中間署名Ｄ１１ｂは送信者の公開鍵Ｄ９で公開鍵暗号化手段８により公開鍵暗号化されたのち受信者の秘密鍵Ｄ１０で公開鍵復号化手段６により要約Ｄ２ｂに公開鍵暗号化される（処理Ｓ１６）。前記中間署名Ｄ１１ｂは共通鍵生成手段１３により共通鍵Ｄ５ｂに変換される（処理Ｓ１４）。前記暗号化データＤ６ｂは該共通鍵Ｄ５ｂで共通鍵復号化手段１１によりデータＤ１ｂに共通鍵復号化され（処理Ｓ９）、該データＤ１ｂは一方向圧縮手段５により要約Ｄ２ｃに一方向圧縮される（処理Ｓ１）。該要約Ｄ２ｃと前記要約Ｄ２ｂは比較手段１２により比較され（処理Ｓ１０）、両者か一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【００３８】以上のような実施の形態８のデータ伝送方法において、送信される署名Ｄ４ａは共通鍵Ｄ５ａを生成する元となる中間署名Ｄ１１ａと異なる内容となるために、受信者の秘密鍵Ｄ１０を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵Ｄ１０で中間署名に公開鍵復号化することかできず、要約を生成てきない。したかって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかてきないため、データＤ１ａの内容は第三者に対して秘匿される。すなわち、受信したデータＤ１ｂを翻訳できるのは、送信者か意図する受信者のみであり、受信者の認証かなされる。さらに、同一内容のデータを複数の受信者に対して伝送する場合、すなわち複数の受信者の公開鍵か互いに異なる場合は、中間署名Ｄ１１ａは受信者ごとに異なる内容て生成されるため、中間署名Ｄ１１ａから生成される共通鍵Ｄ５ａも受信者ごとに異なり、したかって、共通鍵Ｄ５ａて共通鍵暗号化手段７により生成される暗号化データＤ６ａも受信者ごとに異なる。また、送信者の秘密鍵Ｄ３を持たない第三者がデータを改ざんし、改ざんしたデータを一方向圧縮した要約を受信者の公開鍵Ｄ７で公開鍵暗号化しても、送信者の秘密鍵Ｄ３て公開鍵復号化することかてきず、中間署名を生成できないため、署名を生成できない。このため、第三者か改ざんした署名および暗号化データを受信者か受信しても、受信された署名Ｄ４ｂから生成した要約Ｄ２ｂと受信したデータＤ１ｂから生成した要約Ｄ２ｃとを比較すると、両者は一致しない。すなわち、署名Ｄ４ｂから生成した要約Ｄ２ｂとデータＤ１ｂから生成した要約Ｄ２ｃか一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【００３９】

【発明の効果】第１の発明および第２の発明によれば、送信者が送信者自身以外の受信者に対してデータを伝送する場合に、伝送データを共通鍵暗号化して第三者に対して秘匿するために必要な共通鍵は、データから自動的に生成されるため、共通鍵を準備したり、共通鍵を第三者に対して秘匿したり、共通鍵を頻繁に変更するなどの管理が不要となり、共通鍵管理のための作業の必要をなくすことかできる。

【００４０】第３の発明、第４の発明、第５の発明および第６の発明によれば、送信者が送信者自身に対してデータを伝送する場合にも、伝送データを共通鍵暗号化して第三者に対して秘匿するために必要な共通鍵は、データから自動的に生成されるため、共通鍵を準備したり、共通鍵を第三者に対して秘匿したり、共通鍵を頻繁に変更するなどの管理が不要となり、共通鍵管理のための作業の必要をなくすことができる。

【００４１】第７の発明および第８の発明によれば、送信者が送信者自身に対してデータを伝送する場合にも、伝送データを共通鍵暗号化して第三者に対して秘匿するために必要な共通鍵は、データから自動的に生成されるため、共通鍵を準備したり、共通鍵を第三者に対して秘匿したり、共通鍵を頻繁に変更するなどの管理が不要となり、共通鍵管理のための作業の必要をなくすことができる、と同時に、複数の相異なる受信者に同一データを伝送する場合も、受信者ごとに相異なる暗号化データを伝送するため、同一内容か伝送されたことを受信者に対して隠すことができる。

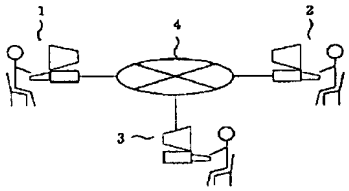
【図面の簡単な説明】

【図１】　この発明の実施の形態１の説明図てある。

【図２】　この発明の実施の形態１、実施の形態２、実施の形態３、実施の形態４および実施の形態５のフローチャートである。

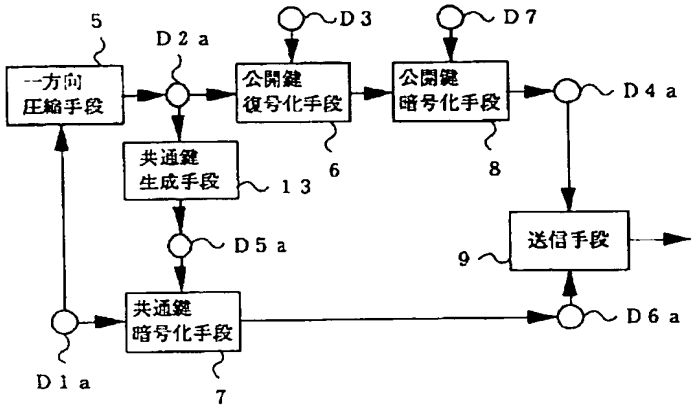
【図３】　この発明の実施の形態２の説明図である。
【図４】　この発明の実施の形態３の説明図である。
【図５】　この発明の実施の形態４の説明図である。
【図６】　この発明の実施の形態５の説明図である。
【図７】　この発明の実施の形態６の説明図である。
【図８】　この発明の実施の形態６、実施の形態７および実施の形態８のフローチャートである。
【図９】　この発明の実施の形態７の説明図である。
【図１０】　この発明の実施の形態８の説明図である。
【図１１】　データ伝送の説明図である。
【図１２】　従来のデータ伝送方法の説明図である。
【図１３】　従来のデータ伝送方法のフローチャートである。
【符号の説明】
１　送信者、２　受信者、３　第三者、４　伝送路、５　一方向圧縮手段、６公開鍵復号化手段、７　共通鍵暗号化手段、８　公開鍵暗号化手段、９　送信手段、１０＊　送信手段、１１　共通鍵復号化手段、１２　比較手段、１３　共通鍵生成手段、Ｄ１　データ、Ｄ２　要約、Ｄ３　送信者の秘密鍵、Ｄ４　署名、Ｄ５　共通鍵、Ｄ６　暗号化データ、Ｄ７　受信者の公開鍵、Ｄ８　暗号化共通鍵、Ｄ９　送信者の公開鍵、Ｄ１０　受信者の秘密鍵、Ｄ１１　中間署名、Ｓ１データから要約を生成する処理、Ｓ２　要約から署名を生成する処理、Ｓ３データを暗号化する処理、Ｓ４　共通鍵を暗号化する処理、Ｓ５　送信処理、Ｓ６　受信処理、Ｓ７　署名から要約を生成する処理、Ｓ８　暗号化共通鍵を復号化する処理、Ｓ９　暗号化データを復号化する処理、Ｓ１０　比較処理、Ｓ１１要約から共通鍵を生成する処理、Ｓ１２　要約から中間署名を生成する処理、Ｓ１３　中間署名から署名を生成する処理、Ｓ１４　中間署名から共通鍵を生成する処理、Ｓ１５　署名から中間署名を生成する処理、Ｓ１６　中間署名から要約を生成する処理。

【図１１】

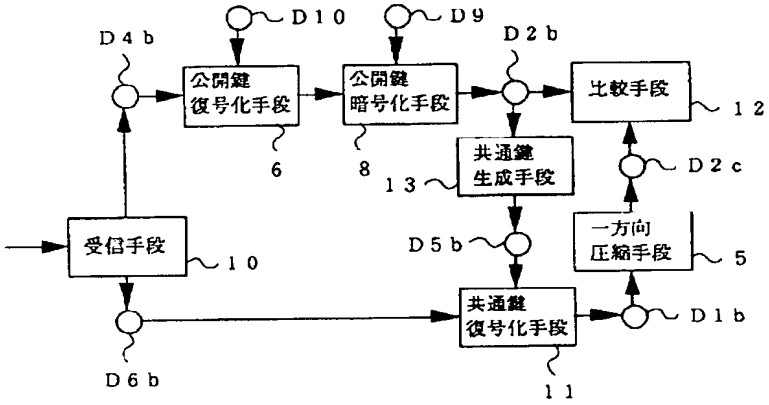


【図1】

(a)

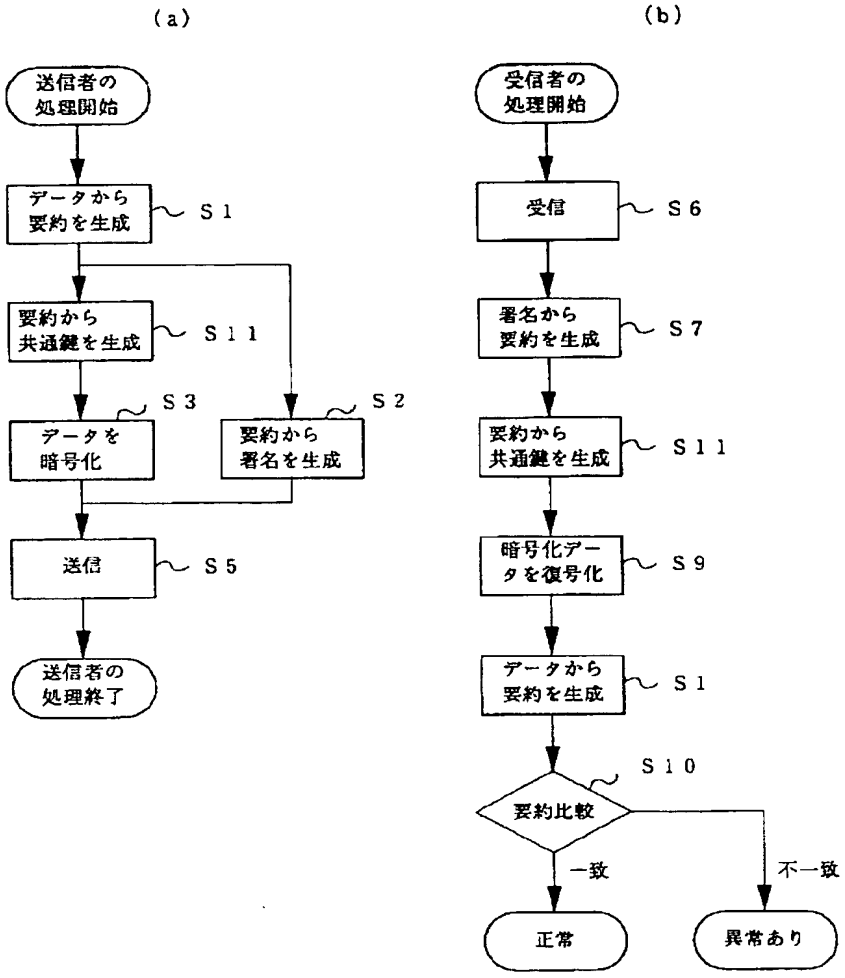


(b)



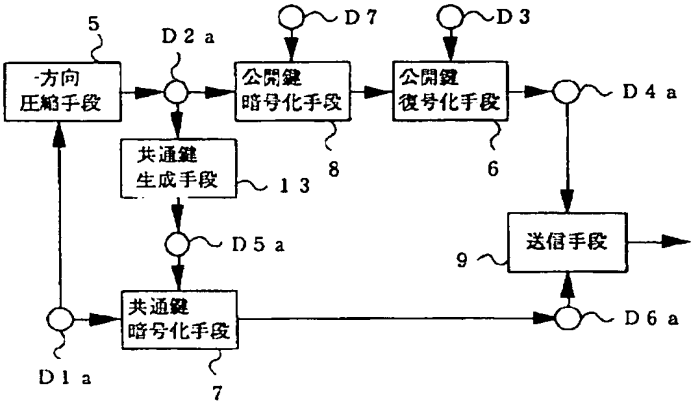
D1－－－データ
D2－－－要約
D3－－－送信者の秘密鍵
D4－－－署名
D5－－－共通鍵
D6－－－暗号化データ
D7－－－受信者の公開鍵
D9－－－送信者の公開鍵
D10－－－受信者の秘密鍵

【図2】

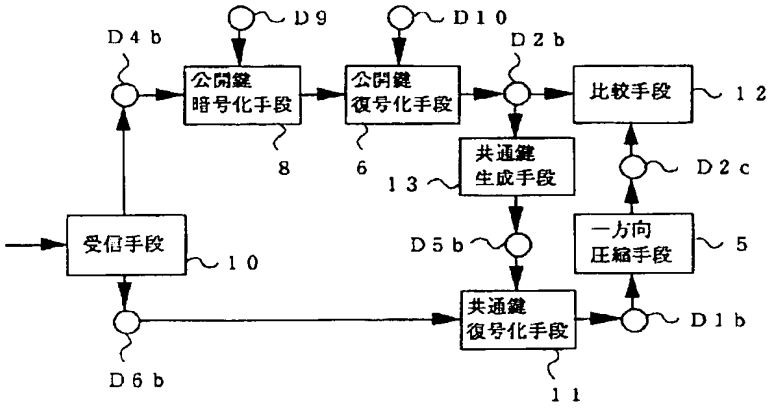

(a)
送信者の処理開始
データから要約を生成
S1
要約から共通鍵を生成
S11
S3
データを暗号化
S2
要約から署名を生成
送信
S5
送信者の処理終了
(b)
受信者の処理開始
受信
S6
署名から要約を生成
S7
要約から共通鍵を生成
S11
暗号化データを復号化
S9
データから要約を生成
S1
S10
要約比較
一致
不一致
正常
異常あり

【図3】

(a)



(b)



D1－－－データ　　D6　－－暗号化データ

D2－－－要約　　D7－－－受信者の公開鍵

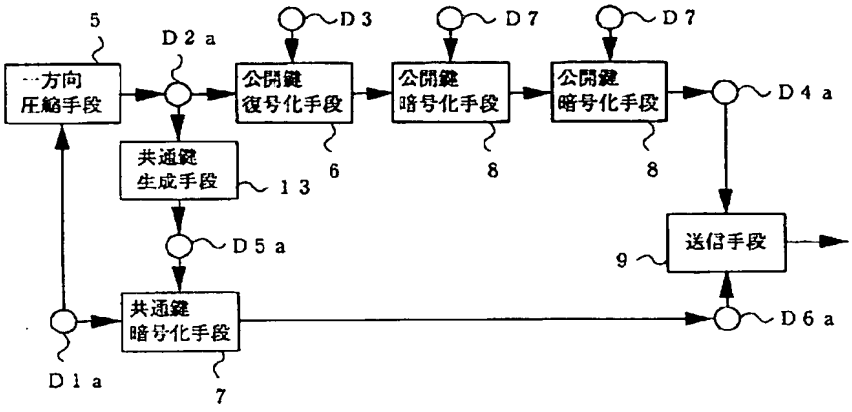
D3－－－送信者の秘密鍵　　D9－－－送信者の公開鍵

D4－－－署名　　D10－－－受信者の秘密鍵

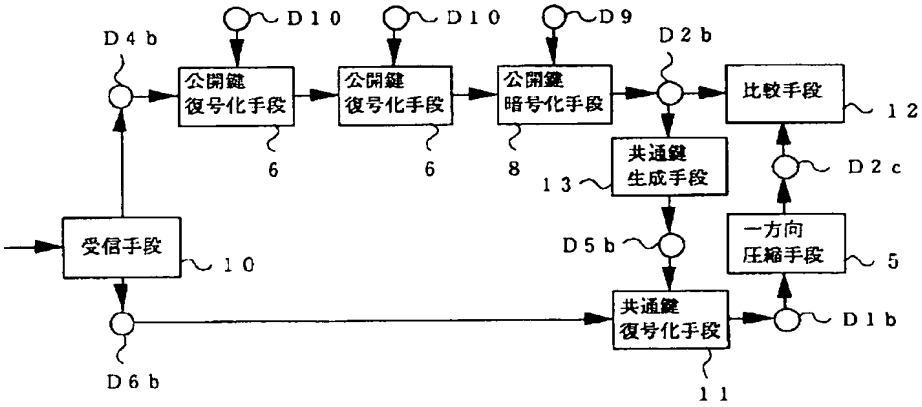
D5－－－共通鍵

【図4】

(a)



(b)



D1－－－データ　　D6－－　暗号化データ

D2－－－要約　　D7－－－受信者の公開鍵

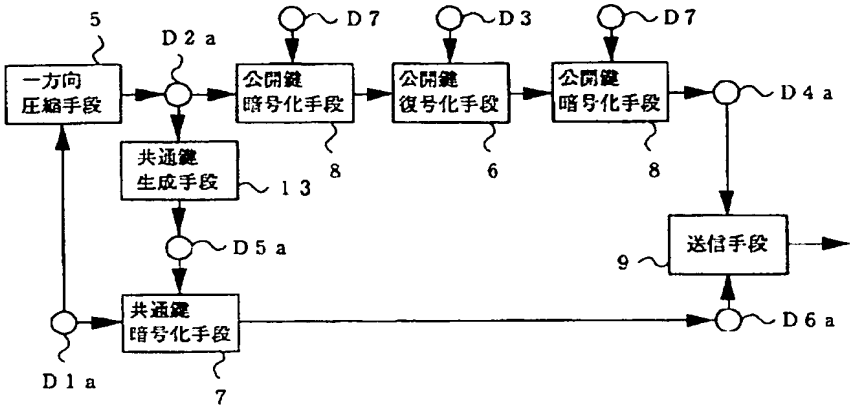
D3－－－送信者の秘密鍵　　D9－－－送信者の公開鍵

D4－－－署名　　D10－－－受信者の秘密鍵

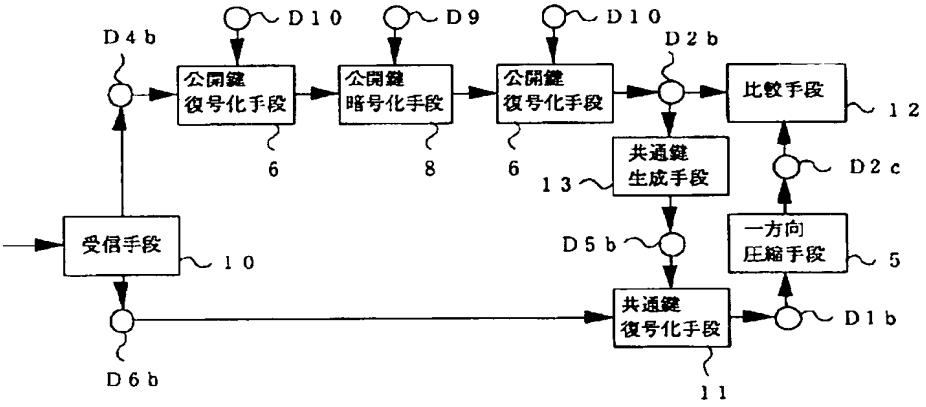
D5－　－共通鍵

【図5】

(a)



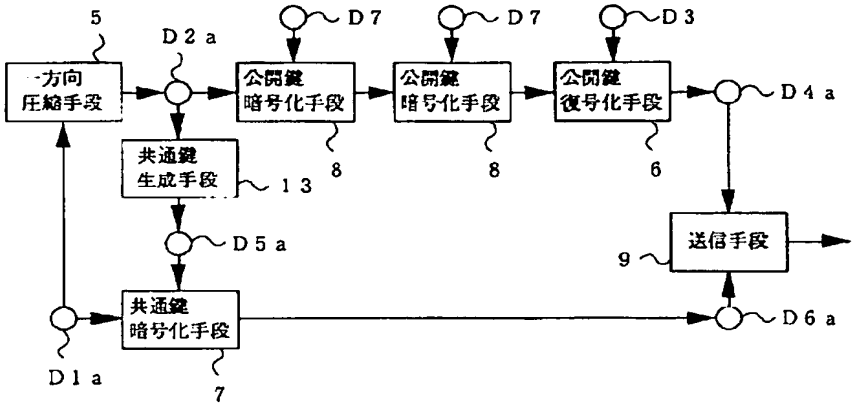
(b)



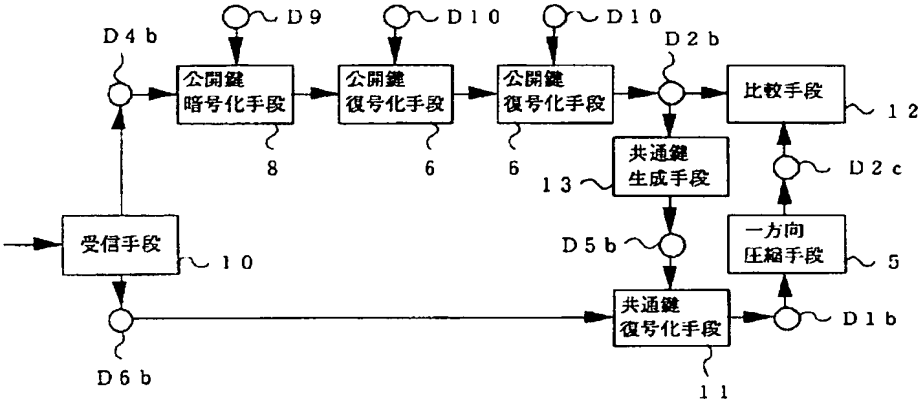
D1－－－データ
D2－－－要約
D3－－－送信者の秘密鍵
D4－－－署名
D5－－－共通鍵
D6－－－暗号化データ
D7－－－受信者の公開鍵
D9－－－送信者の公開鍵
D10－－－受信者の秘密鍵

【図6】

(a)



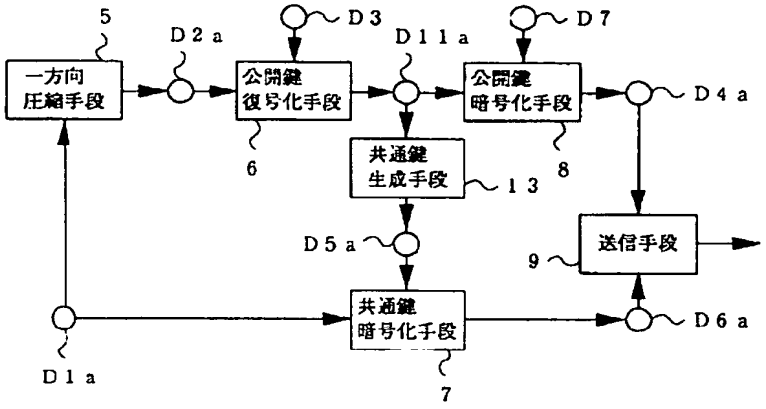
(b)



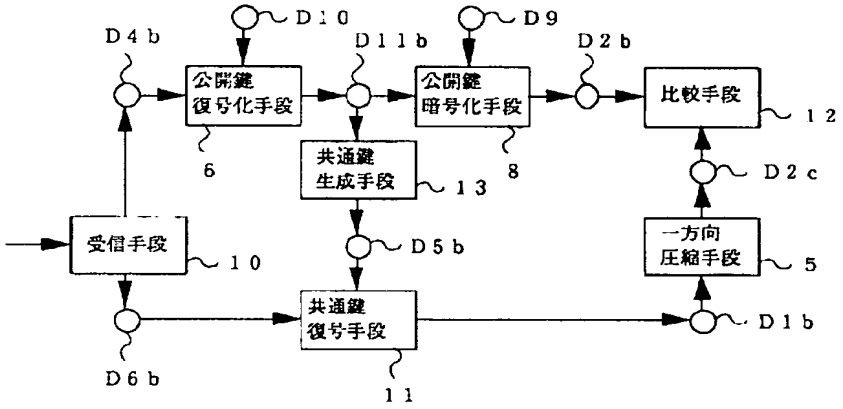
D1－－－データ
D2－－－要約
D3－－－送信者の秘密鍵
D4－－－署名
D5－－－共通鍵
D6－－－暗号化データ
D7－－－受信者の公開鍵
D9－－－送信者の公開鍵
D10－－－受信者の秘密鍵

【図７】

(a)



(b)



D１－－－データ　　D６－－－暗号化データ

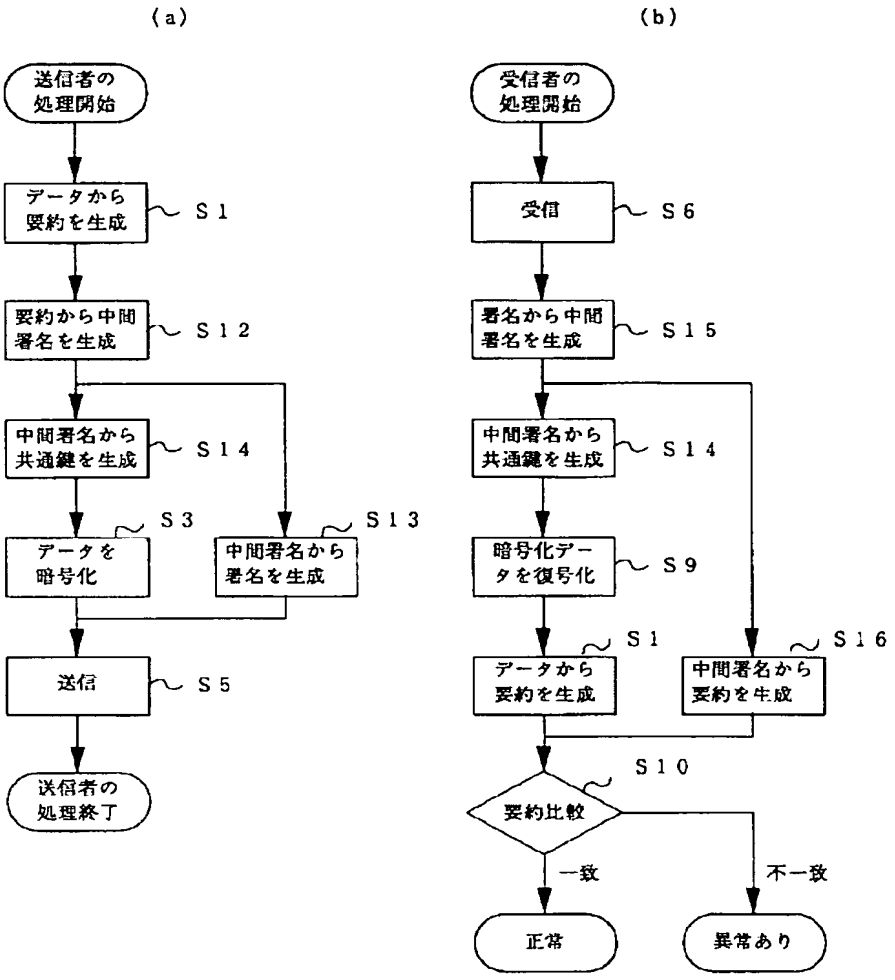
D２　－－－要約　　D７－－－受信者の公開鍵

D３－－－送信者の秘密鍵　　D９－－－送信者の公開鍵

D４－－－署名　　D１０－－－受信者の秘密鍵

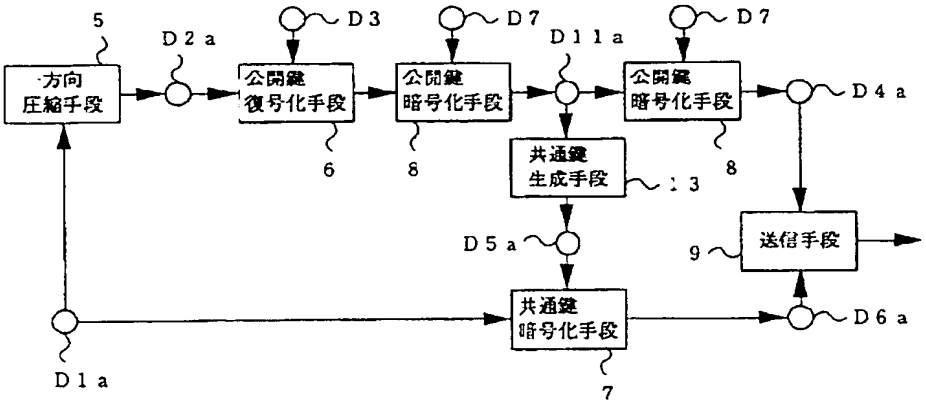
D５－－－共通鍵　　D１１－－－中間署名

【図8】

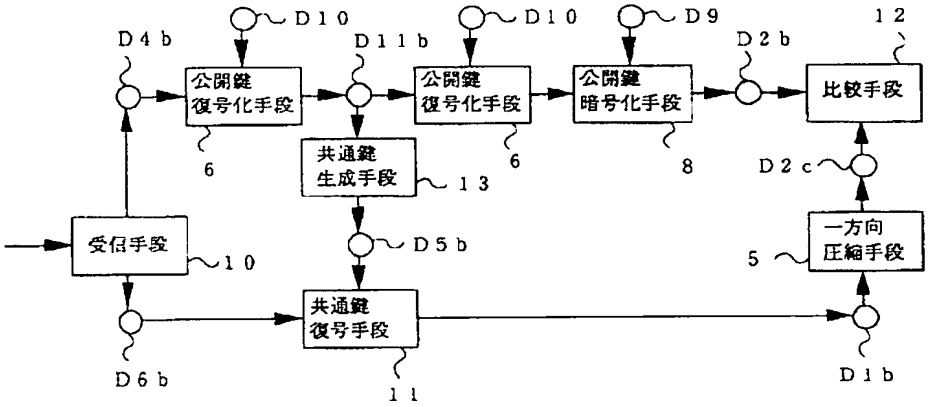

(a)
送信者の処理開始
データから要約を生成
S1
要約から中間署名を生成
S12
中間署名から共通鍵を生成
S14
S3
データを暗号化
S13
中間署名から署名を生成
送信
S5
送信者の処理終了
(b)
受信者の処理開始
受信
S6
署名から中間署名を生成
S15
中間署名から共通鍵を生成
S14
暗号化データを復号化
S9
S1
データから要約を生成
S16
中間署名から要約を生成
S10
要約比較
一致
不一致
正常
異常あり

【図9】

(a)



(b)



D1－－－データ　　D6－－－暗号化データ

D2－－－要約　　D7－－－受信者の公開鍵

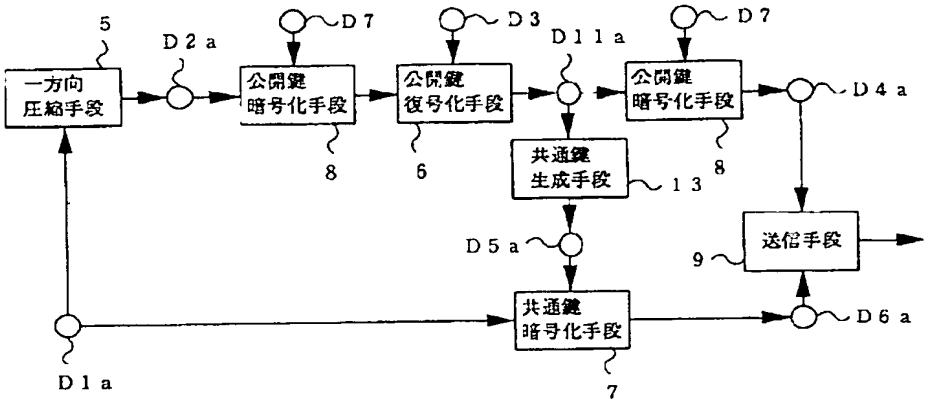
D3－－－送信者の秘密鍵　　D9－－－送信者の公開鍵

D4－－－署名　　D10－－－受信者の秘密鍵

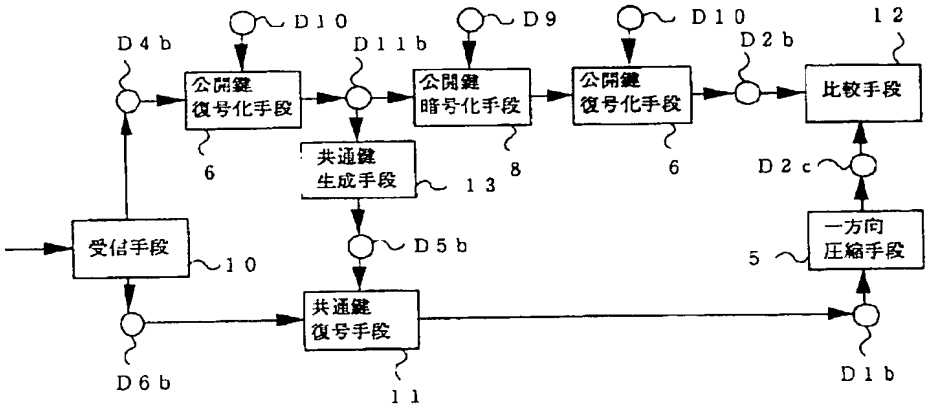
D5－－－共通鍵　　D11－－－中間署名

【図10】

(a)



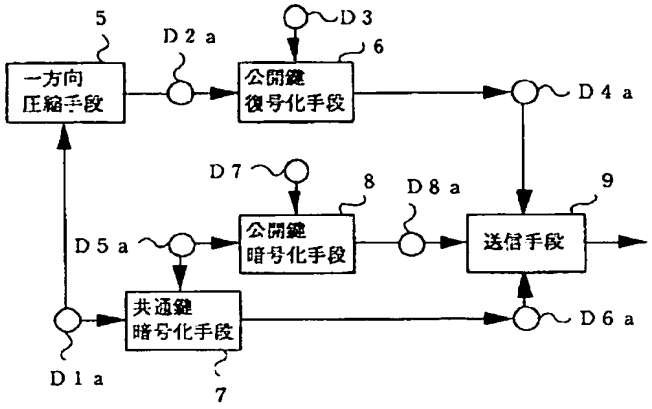
(b)



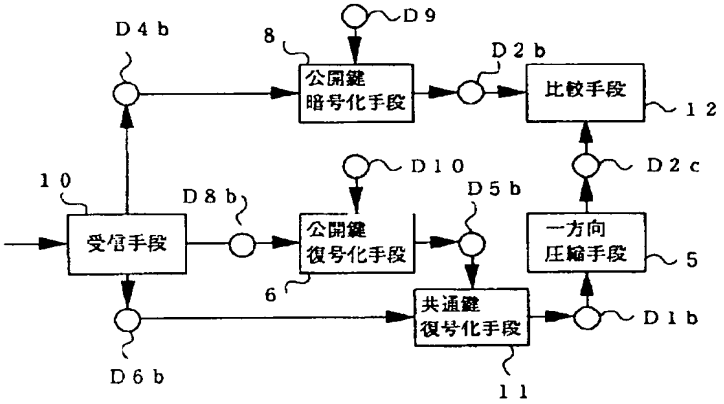
D1－－　データ
D2－－－要約
D3－－－送信者の秘密鍵
D4－－　署名
D5－－－共通鍵
D6－－－暗号化データ
D7－－　受信者の公開鍵
D9－－－送信者の公開鍵
D10－－－受信者の秘密鍵
D11－－－中間署名

【図12】

(a)



(b)



D1－－－データ　　D6　　－暗号化データ

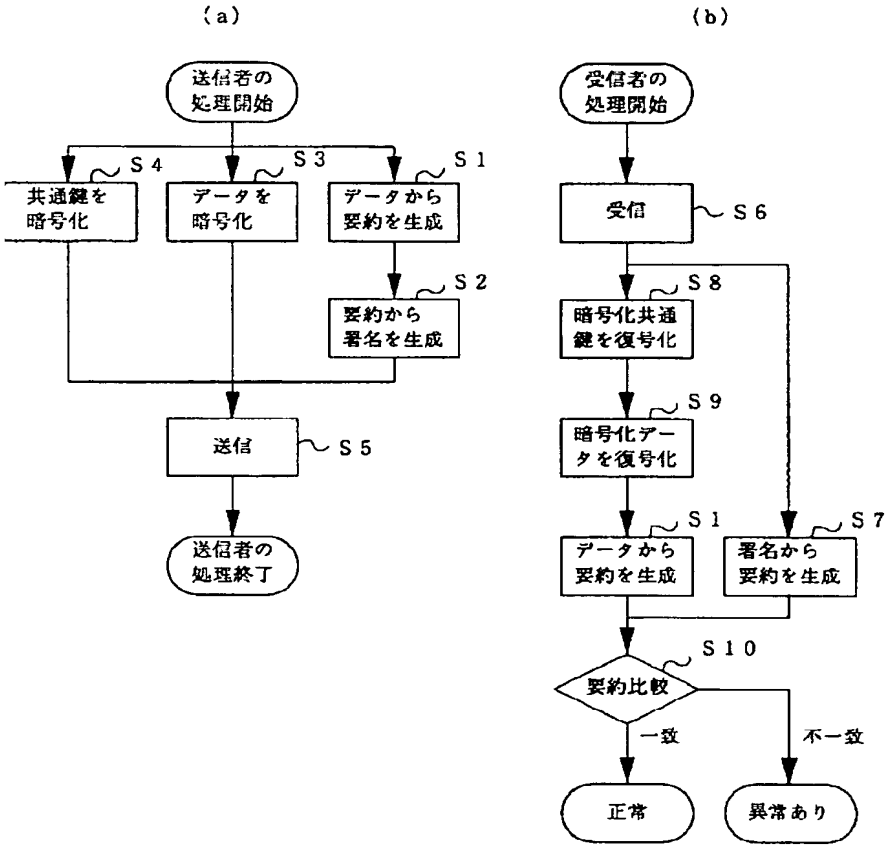
D2－－－要約　　D7－－－受信者の公開鍵

D3－－－送信者の秘密鍵　　D8－－－暗号化共通鍵

D4－－－署名　　D9－－－送信者の公開鍵

D5－－－共通鍵　　D10－－－受信者の秘密鍵

【図１３】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ 9/00	６０１Ｃ	
	9/32				６０１Ｅ	
					６７５Ｂ	